Hack des IT-Rechts: Zu den Folgen des „Doxing-Falls“

Sebastian J. Golla 2019-01-14T09:28:43

Wenn politische Akteure Schäden erleiden, kann dies die Weiterentwicklung des Rechts rasch befördern. So beruht beispielsweise eine der wichtigsten Kodifikationen des Datenschutzrechts in den USA maßgeblich auf der Veröffentlichung der Leihhistorie von Videokassetten des seinerzeit als Richter für den Obersten Gerichtshof nominierten *Robert Bork*. Nun haben die im Dezember 2018 und Januar 2019 bekannt gewordenen Veröffentlichungen von Daten aus dem Privatleben zahlreicher Politiker und Prominenter eine Diskussion über Reformen des IT-Rechts in Deutschland losgetreten. Diese berührt unter anderem das IT-Sicherheitsrecht, das IT-Strafrecht und dessen verfassungsrechtliche Grundlagen.

Schutzpflichten im IT-Sicherheitsrecht

Die Vorfälle werfen zunächst ein Schlaglicht auf das IT-Sicherheitsrecht. Dieses ist bisher fragmentarisch in diversen Fachgesetzen geregelt. Es befindet sich als Rechtsgebiet in einer Findungsphase und ist noch stark von informellen Handlungen und Kooperationen in der Verwaltung geprägt. Die jüngsten Ereignisse dürften die bestehende Tendenz zur Kodifizierung dieses Gebietes antreiben.

Das verfassungsrechtliche Fundament des IT-Sicherheitsrechts ist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welches das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht hergeleitet hat. Wie bereits aus der Formulierung „Gewährleistung“ folgt, hat das „IT-Grundrecht“ neben einer Abwehrkomponente auch einen objektiv-rechtlichen Gehalt. Es besteht eine staatliche Pflicht zum Schutz der IT-Sicherheit und ihrer Grundwerte – der Verfügbarkeit, Vertraulichkeit und Integrität von IT-Systemen. Dabei ist der Schutz der IT-Sicherheit Grundbedingung für den Schutz weiterer Rechte. Im Fall von „Polit-Hacks“ kann dies die Funktionsfähigkeit der Demokratie und die politische Meinungsbildung betreffen, in anderen Fällen sogar Leib oder Leben, wenn es etwa um den Schutz kritischer Infrastrukturen geht.

Die Pflicht zum Schutz der IT-Sicherheit bedarf weiterer Konkretisierungen. Es genügt ihr nicht, wenn der Staat seine Bürger lediglich auf die bestehenden technischen und organisatorischen Möglichkeiten verweist, um die IT-Sicherheit ihrer Systeme selbst zu schützen. Dies würde der Realität der Gefährdungen nicht gerecht werden, zumal es bei Privatpersonen oftmals nicht nur am Gefahrenbewusstsein, sondern auch an dem technischen Sachverstand fehlt, um Gefährdungen wirksam zu begegnen. Um der Schutzpflicht nachzukommen, kann der Gesetzgeber Regelungen zu Organisation und Verfahren der IT-Sicherheit treffen oder Technikgestaltungen vorgeben.

Umgang mit Sicherheitslücken

Ein aktuell besonders relevanter Aspekt der Schutzpflicht ist der Umgang mit IT-Sicherheitslücken. So forderten Politiker angesichts des aktuellen „Datenlecks“ hierfür einerseits Regelungen, die eine Ausnutzung von Sicherheitslücken staatlicherseits einschränken, andererseits aber auch Möglichkeiten für staatliche „Hackbacks“. Dass IT-Sicherheitslücken gravierende Risiken für verschiedene Rechtsgüter bedeuten können, zeigte im Mai 2017 der Fall „WannaCry“: Der US-amerikanische Nachrichtendienst NSA hatte von einer IT-Schwachstelle gewusst, aber weder den Hersteller noch die Öffentlichkeit informiert, sondern eine Infiltrationssoftware auf dieser Grundlage entwickelt. Als Hacker die betreffende Schwachstelle ausnutzten, führte dies unter anderem zu Schäden an kritischen Infrastrukturen.

Auch in Deutschland besteht die Besorgnis, dass staatliche Stellen IT-Sicherheitslücken für Ermittlungszwecke bewusst offenhalten könnten. Den hier bestehenden Zielkonflikt zwischen dem Interesse an dem Offenhalten von IT-Sicherheitslücken zur Gefahrenabwehr bzw. Strafverfolgung und dem Interesse an der allgemeinen IT-Sicherheit thematisierte das Bundesverfassungsgericht bereits im Jahre 2008. Die Bundesregierung hat das Ausnutzen entsprechender Lücken bisher zumindest nicht klar ausgeschlossen.

IT-Schwachstellen in einem weiten Umfang offenzulassen, widerspräche den staatlichen Bekenntnissen, die IT-Sicherheit zu fördern und zu schützen. Mit dem *Paris Call for Trust and Security in Cyberspace* hat sich die Bundesrepublik zuletzt auch einer internationalen Übereinkunft angeschlossen, die die Bekanntmachung und Schließung von IT-Sicherheitslücken unterstützt. Weil es keine bekannte Möglichkeit gibt, die Nutzung dieser Schwachstellen zu kontrollieren, erscheint es mit der staatlichen Pflicht zum Schutz der IT-Sicherheit grundsätzlich unvereinbar, wenn der Staat es unterlässt, IT-Sicherheitslücken zu melden und zu ihrer Schließung beizutragen. Die Befugnisse zur „Online-Durchsuchung“ und Quellen-Telekommunikationsüberwachung werden aus diesem Grund zu Recht in Verfassungsbeschwerden angegriffen.

Zwar sind Fälle denkbar, in denen Interessen an der IT-Sicherheit gegenüber anderen durch die Verfassung geschützten Rechten nach einer Abwägung zurücktreten müssten. Es bedürfte aber mindestens klarer Kriterien für den Umgang mit Schutzlücken, um deren Offenhalten zu rechtfertigen. Solche Kriterien könnten in einem Austausch zwischen potentiell Betroffenen, IT-Herstellern und Nutzern sowie den Sicherheitsbehörden erarbeitet werden. Konkrete Regelungen zum staatlichen Umgang mit Sicherheitslücken könnten sich etwa an die 2017 eingerichtete Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) richten, die Sicherheitsbehörden im IT-Bereich unterstützt und berät. Eine Regelung hierzu könnte in einem Zuge mit der derzeit auf Bundesebene diskutierten allgemeinen Meldepflicht für IT-Sicherheitslücken erfolgen. Dies würde den Schutz der allgemeinen IT-Sicherheit stärken.

Justierungen in der IT-Sicherheitsarchitektur

Das „Datenleck“ hat auch eine Diskussion über die behördlichen Aufgaben und Befugnisse im Bereich der IT-Sicherheit befördert. Zum Schutze der IT-Sicherheit besteht – vor allem auf Bundesebene – eine kaum überschaubare Anzahl von Einrichtungen. Diese sollen sich unter anderem über Gefahren beraten und Abwehrmechanismen entwickeln. Dazu verfügen sie zum Teil über konkrete Abwehrbefugnisse. Die zentrale Behörde zum Schutz der IT-Sicherheit – das BSI – geriet aufgrund ihres Umgangs mit Informationen zum „Doxing-Fall“ in die Kritik.

Es ist zu erwarten, dass die bestehenden behördlichen Strukturen zum Schutz der IT-Sicherheit gestärkt werden. Dies betrifft besonders das beim BSI angesiedelte Nationale Cyber-Abwehrzentrum (NCAZ). Hierbei handelt es sich um eine informelle Struktur ohne exekutive Befugnisse, die als „Informationsdrehscheibe“ verschiedener Bundesbehörden dient. Politisch ist eine Weiterentwicklung des NCAZ schon länger beabsichtigt. Bemühungen zum Schutz der IT-Sicherheit könnten hier noch weiter zentralisiert werden. Vorstellbar wäre es auch, das NCAZ auf eine gesetzliche Grundlage zu stellen.

Zudem dürften die jüngsten Ereignisse den Forderungen des BKA Antrieb geben, neue Befugnisse zur Abwehr von Gefahren im Cyberraum zu erhalten. Diese sollten sich nach BKA-Präsident *Holger Münch* an bestehenden Befugnissen zur Abwehr von Gefahren des internationalen Terrorismus orientieren. Dafür bedürfte es einer mit Art. 73 Abs. 1 Nr. 9a GG vergleichbaren Regelungskompetenz. Diese Forderung entspricht einer allgemeinen Tendenz, sicherheitsbehördliche Aufgaben und Befugnisse angesichts technologischer Entwicklungen zu zentralisieren. Waren es im 19. Jahrhundert Fortschritte in Technik und Verkehrswesen, die zu der Forderung zentraler polizeilicher Einrichtungen führten, um gegen „reisende Verbrecher“ vorzugehen, sind es heute Handlungen von Straftätern im virtuellen Raum. Bei einer Stärkung der Befugnisse des BKA wären allerdings auch die geschilderten Zielkonflikte zu beachten, die etwa im Zusammenhang mit dem Offenhalten von Sicherheitslücken bestehen. Die Tätigkeiten des BSI, die die allgemeine IT-Sicherheit stärken, sollten mindestens ebenso gefördert werden.

Schärfung des IT-Strafrechts

Die aktuellen Ereignisse haben zudem dazu geführt, dass Strafbarkeitslücken im IT-Strafrecht behauptet und höhere Strafen für die missbräuchliche Verwendung von Daten gefordert werden. Diese Forderungen sind mit Vorsicht zu genießen. Das IT-Strafrecht weist insgesamt eine Tendenz zur symbolischen Expansion auf. Dies zeigen sowohl der misslungene Tatbestand der Datenhehlerei (§ 202d StGB), gegen den noch eine Verfassungsbeschwerde anhängig ist, als auch das Vorhaben einer ausufernden Strafbarkeit für den „digitalen Hausfriedensbruch“.

Echte Strafbarkeitslücken für die Veröffentlichung personenbezogener Daten sind angesichts der äußerst weit gefassten Straftatbestände des Bundesdatenschutzgesetzes (§ 42 BDSG) kaum zu erkennen. Diese stellen

unter anderem das unberechtigte Veröffentlichen personenbezogener Daten mit Schädigungsabsicht unter Strafe. Dafür reicht ein sicheres Wissen um den Eintritt eines Schädigungserfolges aus, der in immateriellen Nachteilen durch Ehrverletzungen und Bloßstellungen bestehen kann. Ein solches Wissen dürfte bei der massenhaften Veröffentlichung privater Informationen von Politikern und Prominenten über Twitter vorgelegen haben.

Allerdings ist zuzugeben, dass das Datenschutzstrafrecht nicht auf den spezifischen Unwertgehalt einer bloßstellenden Veröffentlichung zugeschnitten ist, wie sie durch das so genannte Doxing erfolgt. Dies gilt ebenso für den – neben den Vorschriften des BDSG grundsätzlich überflüssigen – Straftatbestand der Datenhehlerei. Anstelle der Straftatbestände des BDSG, die im Nebenstrafrecht ein Schattendasein führen, wäre es sinnvoll, im StGB spezifische Risiken für das Persönlichkeitsrecht durch den Missbrauch von Daten in den Blick zu nehmen. Die Diskussion sollte sich dabei aber nicht an angeblichen Strafbarkeitslücken aufhängen, sondern mit dem Ziel eines zeitgemäßen Zuschnitts des IT-Strafrechts unter besonderer Beachtung der rechtsstaatlichen Gebote von Bestimmtheit und Verhältnismäßigkeit geführt werden.

Lehren für die Diskussion um die Strafbarkeit des Doxing lassen sich auch aus der Diskussion um ein allgemeines Indiskretionsdelikt ziehen. Von Beginn des 20. Jahrhunderts bis in die 1970er-Jahre wurde überlegt, eine weite Strafbarkeit für Fälle der Offenbarung persönlicher Informationen im StGB einzuführen. Die Regelungsvorschläge waren vor allem von technischen Fortschritten angetrieben, die es ermöglichten, Informationen massenhaft zu verbreiten. Die Entwürfe zur Schaffung eines solchen Deliktes setzten sich allerdings unter anderem wegen Zweifeln an ihrer Bestimmtheit sowie Problemen bei der Abgrenzung von den Ehrschutzdelikten nicht durch. Ebenfalls bedenklich erschien ihre Vereinbarkeit mit dem „*ultima ratio*“-Prinzip angesichts weitgehender zivilrechtlicher Sanktionsmöglichkeiten für Indiskretionen. Diese grundlegenden Bedenken bestehen heute fort, so dass eine Diskussion um ein allgemeines Indiskretionsdelikt 2.0 vermieden werden sollte. Denkbar wäre aber etwa eine spezifische Ergänzung bestehender Regelungen wie der Strafbarkeit der Nachstellung, die auch eine Tatbestandsvariante der missbräuchlichen Verwendung personenbezogener Daten hat (§ 238 Abs. 1 Nr. 3 StGB).

Fazit

Der „Doxing-Fall“ und die damit ausgelösten Diskussionen dürften den Prozess der Entwicklung des IT-Sicherheitrechts beschleunigen. Gelingt es, die grundrechtliche Schutzpflicht überzeugend gesetzlich zu konkretisieren, könnte dies einen echten Gewinn für die IT-Sicherheit bedeuten. Dabei ist freilich im Blick zu behalten, dass rechtliche Regelungen nur einer von vielen Bausteinen sind, um die IT-Sicherheit zu stärken. Zu warnen ist vor einer reflexartigen Verschärfung des IT-Strafrechts, die nicht nur negative Folgen für „White-Hat-Hacker“, sondern auch für die Ausübung von Presse- und Meinungsfreiheit haben könnte. Ob es dem 20-jährigen Schüler aus Hessen gelungen ist, die Entwicklung des IT-Rechts zu „hacken“ und zu einer Evolution zu führen, die vielleicht sogar berechtigten Anlass dazu gibt, „stolz“ auf

diesen jungen Mann zu sein, wird sich in den nächsten Monaten und Jahren zeigen müssen.
